enforcement will lose access to the information in a digital environment, because digital switching prevents law enforcement from having the same access to the intercept hardware or location that it has today.

63. Absent a message indicating that the subject has pressed one of the feature keys or the flash hook, law enforcement will be presented with potentially severe investigative, evidentiary, and prosecutorial problems. Law enforcement may be unable to determine what has happened to a call when the call dramatically changes for no apparent reason. For example, a subject who is engaged in criminal conspiracy with two associates may use his flash hook capability to move back and forth rapidly between the two associates in two concurrent call legs. Without the receipt of a message showing the "flash" event, law enforcement may be unable to follow the course of the conversation or determine to whom the subject is speaking at any point in the conversation.

64. In addition, law enforcement will be left with an incomplete and potentially inaccurate evidentiary picture of the subject's dialing and signaling activities incidental to his calls. The absence of messages indicating dialing or signaling that significantly changes the call would undermine the ability of law enforcement to present critical evidence and testify in court on such fundamental matters as whether the subject was still involved in the call at a particular time; if so, in what fashion; and if not, what happened to the call.

---

equivalent signaling is done via data messaging.

65. CALEA was enacted to prevent the loss of such critical information and evidence. Industry has suggested that dialing and signaling beyond the digit keys and feature codes initiating a call are not "call-identifying information." However, a subject's dialing and signaling inputs during a call that control services like call forwarding and call transfer come squarely within CALEA's definition of "call-identifying information," for they constitute "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2). As explained above, without this signaling information, law enforcement will be unable to identify the destination of each communication. Moreover, CALEA's legislative history makes clear that CALEA was intended "to preserve the government's ability * * * to intercept communications involving * * * features and services such as call forwarding, speed dialing, and conference calling * * * ." House Report at 9. The interim standard is fundamentally deficient in this regard.

66. The interim standard also excludes information about another important kind of subject-initiated dialing and signaling activity: "post-cut-through" dialing. In long distance calls, credit card calls, and (in some instances) local calls, the dialing and signaling information necessary to complete a call and reach the intended party frequently occurs after the "cut-through."[16] For example, when

[16] "Cut-through" means the completion of a connection in one direction (partial), or both directions (full), between two call appearances. See Appendix 1 (§ 64.1702). There are two communications paths that must be connected in order for one party to communicate with another party through a telephone switch: the forward talk path and the reverse listen path. Normally, when a call is set up, the caller's reverse listen path is connected to the called party's talk path first, because often the "called party" is an additional switch which may put a busy signal or some announcement on that path. That is referred to as "partial cut-through." When the second switch provides an answer signal to the first switch, because the called party answered or the second switch needs to

using a credit card, a subject may dial through one service (X) to the carrier's (Y's) 800-number service and will then be prompted to continue dialing the telephone number to reach the party being called (i.e., the destination of the call). The numbers dialed are then transmitted over X's equipment, facilities, and services to reach the called party. The numbers dialed after the connection is made to Y's service occur after the "cut-through." Thus, the destination of the call is revealed only by the numbers dialed after the cut-through.

67. The interim standard does not require carriers to provide law enforcement with access to post-cut-through dialing information. Under the interim standard, therefore, law enforcement will not have access to digits dialed after the call is connected. This is information which law enforcement traditionally received in the pre-CALEA POTS environment.[17] Without this information, law enforcement will be unable to determine the destination of some subscriber-initiated calls.

68. The inability to obtain post-cut-through dialing information creates obvious investigative and evidentiary problems. For example, law enforcement agents may find it substantially more difficult,

---

collect additional digits to route the call, the first switch will connect the caller's forward talk path to the called party's listen path. When both paths are connected it is called "full cut-through."

[17] In the analog era, law enforcement obtained information via pulses and tones, which were signaled across the analog local loop to which law enforcement was directly connected. Much of this information is now digitized and therefore not capable of being interpreted by law enforcement through use of a pen register. In addition, information regarding many relatively new features does not pass through to the local loop, but remains accessible only in the switch.

if not impossible, to establish the identity of the party to whom the intercept subject is speaking if they are unable to identify the phone number associated with that party. Thus, in an illegal drug case, law enforcement might be unable to link a drug distributor with the source of his drugs. Similarly, in a child pornography case or other case in which a subject uses the telephone to contact buyers, law enforcement might be limited to the arrest of a single subject rather than all participants, because law enforcement would only have information about which long distance company the subject was using -- not the subsequent post-cut-through digits that would have identified the called parties.[18]

69. A carrier's failure to provide law enforcement with all of the subject's dialing, including post-cut-through dialing, amounts to a failure to provide law enforcement with the number of the party that the subject actually called. The failure to mandate access to all dialing and signaling information necessary to complete the call therefore renders the interim standard fundamentally and critically deficient under Section 103 of CALEA. Under CALEA's definition of call-identifying information, post-cut-through dialing and signaling information that completes a call is "signaling information" that identifies the "destination" of the call. 47 U.S.C. § 1001(2). Omission of this information conflicts with the carrier's basic obligation under Section 103(a)(2) to "isolat[e] and enabl[e] the government * * * to access call-identifying information that is reasonably available to

---

[18] Even if law enforcement could eventually obtain the post-cut-through dialing information from the long distance carrier, it would not be accessible in a timely fashion, so as to permit the dialing to be associated with the call content, as required by Section 103(a)(2)(B) of CALEA (47 U.S.C. § 1002(a)(2)(B)). Moreover, a subject could change to a new long distance carrier at the beginning of each call.

the carrier." Id. § 1002(a)(2). It also conflicts with the additional obligation to ensure that call-identifying information is provided "in a manner that allows it to be associated with the communication to which it pertains." Id. § 1002(a)(2)(B).

70. Industry has suggested that its obligation under Section 103 of CALEA ends once a call effort connects, for example, to an 800 calling card service. Law enforcement believes that the Commission has addressed this issue and concluded otherwise. The Commission has recognized that a call is not "completed" when it connects to an 800 calling card service, but rather when it connects to the called party.[19] Under CALEA, therefore, the "call-identifying information" that must be associated with a "communication" includes all dialing required to complete the call.

71. CALEA does not draw any distinction between pre-cut-through and post-cut-through dialing or signaling information used to process, direct, or complete a call. Nor is there any privacy-based constraint under CALEA, the pen register statutes, or the Constitution that prevents a carrier from providing all such dialing information, whether pre-cut-through or post-cut-through.[20] Congress was aware that federal officials have long obtained all dialing information of a criminal subject, including

---

[19] See FCC Report and Order, In re Implementation of the Pay Telephone Reclassification and Compensation Provisions of the Telecommunications Act of 1996, Docket No. 96-388 (Sept. 20, 1996), at 33 ("a 'completed call' is a call that is answered by the called party").

[20] See United States v. New York Telephone Co., 434 U.S. 159 (1977) (dialing information obtained by a pen register device does not constitute the contents of a communication requiring a Title III court order); Smith v. Maryland, 422 U.S. 735 (1979) (no Fourth Amendment protection for dialing information).

post-cut-through dialed numbers, pursuant to pen registers executed in the "local loop," and Congress expressed no intention in CALEA to change this capability. Without such information, law enforcement will be unable to determine the destination of subject-initiated calls. Therefore, access to post-cut-through dialing information is required under CALEA and should be incorporated into technical requirements and standards established by the Commission.

72. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing law enforcement with access to all subject-initiated dialing and signaling, including the use by a subject of flash hooks, feature keys, and all other key usage." Appendix 1 (§ 64.1708(c)). The proposed rule further provides that carriers "shall ensure that their equipment, facilities, or services are capable of extracting the digits dialed by the subject following cut-through at the access point and delivering those digits to the law enforcement agency in a post-cut-through InBandsDigit message containing those digits." Id. (§ 64.1708(i)).

73. (ii) Information on participants in a multi-party call. A subscriber may subscribe to services or features that would support a multi-party call. If so, various associates can be added to, placed on hold during, or dropped from a call. The interim standard does not require carriers to provide any signaling information or message indicating that a party has joined a call, been placed on hold, or dropped from a call. The exclusion of this information from the interim standard will deprive law enforcement of important investigative and evidentiary information to which it is lawfully entitled.

74. Law enforcement seeks the delivery of three messages that would provide it with access to information about which parties are participating in a call. A "party hold" message would be generated when any party is placed on hold by the intercept subject. A "party join" message would be generated when (1) one or more parties previously placed on hold are added to the current call or (2) a party joins an existing call with an intercept subject. A "party drop" message would be generated when a party is released from a multi-party call and the call continues among two or more other parties.

75. Party hold, party join, and party drop messages enable law enforcement to identify who is connected in a subject's conference call at any point in the conference. Knowledge of when participants join or depart a call enables law enforcement to identify the source and recipient of each communication within a conferenced call. Without these messages, law enforcement would not know who joins or leaves a conference call, whether the subject alternated between calls, or which parties heard or said parts of a conversation. Such information can be critical for investigatory purposes, particularly in conspiracy cases. For example, if an organized crime leader issues instructions to carry out a murder in the course of a multi-party call, and law enforcement cannot tell which of a number of conferenced associates were participating in the conversation at the time, it may be substantially more difficult to prevent the murder from taking place.

76. In addition, incomplete call-identifying information prevents the collection of evidence that parties remained on a call after they first joined. Thus, if a party remains silent, a law enforcement agency executing a Title III interception order has no way of demonstrating that the party heard

significant portions of the communication. The lack of such evidence may allow doubt to be raised as to whether a party participated in all communications in a call and may jeopardize prosecutions based on that evidence.

77. In the analog environment, law enforcement obtained, pursuant to pen register orders, signaling information indicating that a subject joined other participants in a multi-party call. However, law enforcement was unable to obtain information that a particular participant was placed on hold during, or dropped from, a multi-party call, because such information resided within, and required access to, the switch. Law enforcement could therefore identify the range of participants who might be involved in a multi-party call, but would have to infer specifically which participants heard portions of the call. CALEA's definition of "call-identifying information" now obligates carriers to provide this information.

78. Industry has suggested that party join, party hold, and party drop messages do not constitute "call-identifying information" as that term is defined by CALEA. However, Congress chose to define "call-identifying information" as dialing or signaling information that is specific to "each communication" generated or received by a subscriber. 47 U.S.C. § 1001(2). When calls placed to or by a subject are affected by triggering the joining, holding, and releasing of parties, each function essentially has the same fundamental purpose and effect -- it controls the "direction," "destination," or "termination" of the communication of each "leg" of the call. Information that enables law enforcement to identify the destination of a call or to understand its status thus falls squarely within CALEA's definition of call-identifying information. Ibid. The interim standard's failure to include

party join, party hold, and party drop messages therefore renders it deficient under Section 103 of CALEA.

79. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing messages to law enforcement that enable law enforcement to identify the parties to a conversation at all times." Appendix 1 (§ 64.1708(b)). The proposed rule defines specific requirements and parameters for "party join," "party hold," and "party drop" messages. Id. § 64.1708(b)(1)-(9).

80. (iii) Access to all network-generated in-band and out-of-band signaling. When a call attempt is sent to or from a subscriber's service, it produces network-generated signals such as ringing, busy signals, or a call waiting signal. These signals may be either "in-band" (transmitted over the same circuit as the communication) or "out-of-band" (transmitted over a separate circuit). For subject-originated call attempts, such signals indicate whether the subject ends a call because the associate's line is ringing, busy, or before the network could complete the call to the associate. For incoming call attempts to the subject, the signals indicate whether the subject's telephone was alerted by tones, a visual indicator, or by a text message. Signaling information generated by call attempts has both investigatory and evidentiary significance for law enforcement. For example, criminals may use ringing signals as a way of conveying pre-arranged messages to each other without having to engage in direct conversations over the phone system.

81. The interim standard does not require carriers to provide law enforcement with notification of network-generated call progress signals. This omission is inconsistent with the requirements of Section 103(a)(2) of CALEA, for despite industry's apparent contrary view, such signaling falls squarely within CALEA's definition of "call-identifying information." Call-identifying information includes "signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber * * * ." 47 U.S.C. § 1001(2) (emphasis added). A call attempt may "terminate" with ringing (without an answer), a busy tone, or a trunk busy signal; signaling such as this conveys information on call termination and therefore constitutes call-identifying information. Similarly, a network-generated call-waiting tone or a "stutter" dial tone (which indicates that a call was redirected to a voice mail system and a voice mail message was recorded) would identify the "direction" or "destination" of a call, and would therefore constitute call-identifying information. In short, CALEA requires carriers to provide law enforcement with any signaling information indicating how the network treated a call attempt: whether or not it was completed, how the call may have been redirected or modified, and how the call ended. This information historically has been available to law enforcement on call content channels; stutter dial tones and other tones are audible signals sent to the subscriber over the local loop, to which law enforcement has access. However, digital switching and new technology have given rise to network-generated call progress messages that are not available over call content channels.

82. The proposed rule provides that carriers "shall ensure that their equipment, facilities, or services are capable of providing notification messages to law enforcement over the CDC [call data

channel] of in-band and out-of-band signaling from the subscriber's service throughout each call." Appendix 1 (§ 64.1708(d)). The rule provides that notification messages "shall be triggered and delivered to the law enforcement agency to report out-of-band signaling delivered through a subscriber's service that can be sensed by the subject and to report in-band signaling applied by the equipment, facilities, or services supporting the subscriber's terminal." Ibid. The rule also defines specific requirements and parameters for notification messages. Id. § 64-1708(d)(1)-(3).

83. (iv) Delivery of call-identifying information on call data channel. In the interim standard, industry proposes to deliver certain call-identifying information over "call data" channels or circuits that would be separate from the "call content" channels or circuits that deliver intercepted communications. However, industry has suggested that other call-identifying information, such as the post-cut-through digits described above, need not be provided over the call data channel, but that law enforcement instead should extract that information from a separately leased call content channel.

84. Industry contends that Section 103 does not mandate delivery over a call data channel of call-identifying information that is capable of being extracted from the call content channel. We agree that a carrier could comply with its delivery obligations under Section 103 without delivering this information in this fashion.[21] However, CALEA contemplates that carriers will employ the most efficient and effective means of delivering authorized surveillance information to law enforcement.

---

[21] As industry appears to recognize, certain call-identifying information must be delivered over a call data channel because it is not available on a call content channel.

See, e.g., 47 U.S.C. §§ 107(a)(1) (requiring consultation between law enforcement and industry "[t]o ensure the efficient and industry-wide implementation of the assistance capability requirements of section 103") (emphasis added); id. § 109 (addressing recovery of costs incurred to establish the capabilities required by Section 103). Having two separate channels to access and process call-identifying information would result in a substantial and unnecessary duplication in equipment, facilities, and cost. Unless all call-identifying information is delivered over a call data channel, law enforcement would be required, for the execution of a pen register order alone, to procure both a call data channel and a call content channel to ensure delivery of all of the dialing activity used to complete or control a call, even though that information could easily be delivered over a single call data channel. This kind of duplication of effort and expense is inconsistent with the spirit and purposes of CALEA.

85. A more cost-effective solution is to specify that all call-identifying information, including all dialed digits, be delivered to law enforcement over the call data channel. Requiring that appropriate call-identifying information be delivered over a call data channel or circuit is consistent with the legislative purpose of providing law enforcement with the information in the most efficient and effective means reasonable. In addition, delivering call-identifying information over a call data channel minimizes the risk of inadvertent intrusions on call content when the government is seeking only call-identifying information. It thus furthers the carriers' responsibilities under Section 103(a)(4)(A) of CALEA (47 U.S.C. § 1002(a)(4)(A)) to provide access to call-identifying information "in a manner that protects * * * the privacy and security of communications and call-identifying information not authorized to be intercepted." For these reasons, the proposed rule

provides that carriers shall deliver post-cut-through dialed digits and notification messages for in-band and-out-band signaling over the call data channel. Appendix 1 (§ 64.1708(d). (i)(1)).

86. (c) Timely delivery of call-identifying information. Section 103(a)(2)(A) of CALEA (47 U.S.C. § 1002(a)(2)(A)) obligates carriers to provide law enforcement with access to call-identifying information "before. during, or immediately after the transmission" of the communication to which it pertains. or "at such later time as may be acceptable to the government." In addition. Section 103(a)(2)(B) requires that call identifying information be made available "in a manner that allows it to be associated with the communication to which it pertains." A carrier relies on dialing and signaling information associated with a particular call in order to process and control that call from origin to destination and termination. including any redirection signaled during the call.

87. Law enforcement currently acquires contemporaneous information regarding the processing and content of a call through its monitoring of the local loop. It is imperative for law enforcement to be able to associate the call-identifying information to the call to which it pertains in an expeditious manner so that law enforcement can promptly and accurately correlate relevant evidence. and respond in emergency and life-threatening cases. Assume. for example. that the subject places a call to a "contract killer." and that the call involves a murder that is to take place immediately. If. while intercepting the "contract murder" communication. law enforcement cannot immediately associate the call-identifying information with the communication. law enforcement officers may be unable to save a life because they are not able to identify promptly. through the acquisition of the

telephone dialing information. whom the subject had called and where that party's telephone was located.

88. The prompt receipt of call-identifying information is also critical. for example. in illegal gambling cases. where the subject typically uses a "flash hook" feature to continuously accept incoming calls being held on "call-waiting." Without expeditiously receiving the call-identifying information. law enforcement would be unable to identify the separate calls.

89. The prompt receipt of call-identifying information that is clearly associated with a particular communication is also critical for law enforcement to carry out its statutory obligation of "minimizing" the interception of non-criminal communications to promote privacy. See generally 18 U.S.C. § 2518(5). To carry out its minimization obligations. law enforcement must quickly identify all parties to a conversation, even in multi-party calls. to determine the criminal culpability of the parties to the call. If a subject makes a call to a known non-culpable person or entity, such as a relative or business that is known not to be involved in criminal activity, law enforcement should immediately minimize the interception. In a multi-party call. if a subject drops off the call or an additional subject joins the call. law enforcement must promptly recognize that these events have occurred. ascertain which subjects are party to the call. and determine what. if any, minimization procedures should be employed. Without the prompt receipt of call-identifying information these requirements cannot be met.

90. Despite the importance of prompt delivery of call-identifying information, the interim standard places no requirements on when call data is to be delivered to law enforcement. The interim standard therefore would permit carriers to deliver call-identifying information at a time other than "before, during, or immediately after" the communication -- and consequently would threaten law enforcement's traditional ability to associate call-identifying information with the communication to which it pertains. The failure of the interim standard to impose a specific delivery time requirement renders it manifestly deficient under Section 103(a)(2) of CALEA.

91. CALEA does not specify a particular time frame that would satisfy the "association" requirement of Section 103(a)(2)(B). However, the establishment of a reasonably short and objective timing requirement is essential to effectively implement that requirement and to ensure that call-identifying information is, in fact, delivered "before, during, or immediately after" a communication.

92. The proposed rule provides that carriers shall access and deliver call-identifying information to law enforcement "contemporaneously with the communications to which it pertains, or in a manner comparable to the speed with which other signaling messages are sent in the public network so that call-identifying information may be associated with the related communications." Appendix 1 (§ 64.1708(e)). Consistent with carrier network processing of call-identifying information, the proposed rule specifies an accuracy rate of 100 milliseconds (ms) for time stamps (i.e., no more than 100 ms difference between the time of the event and the time recorded in the time stamp) and

delivery "in as near real time as possible, but no later than three seconds after the occurrence of the associated call event * * * ." Id. § 64.1708(e)(1)-(3).

93. The particular timing requirements in the proposed rule are not the only ones that would satisfy Section 103(a)(2). Nevertheless, either these requirements or other reasonable and comparably effective ones are necessary. Adoption of such requirements will enable call data to be associated with the correct call and will permit law enforcement to react quickly in situations where innocent lives are threatened. For example, when a ransom call or a bomb threat call is made, the calling number will be provided quickly and will give law enforcement an opportunity to prevent harm to potential victims that would not be available if the interim standard's lack of timing requirements were left unaltered.

94. **(d)** Automated delivery of surveillance status information. Action by the Commission is also warranted with respect to the delivery of surveillance status information. Section 103 of CALEA provides that a telecommunications carrier "shall ensure" that its equipment is capable of intercepting communications and isolating call-identifying information. Section 103 thereby places an affirmative obligation upon the carrier to verify that its equipment is operational and that law enforcement has access to all communications and information within the scope of the authorized surveillance.

95. Any other interpretation of Section 103's "ensure" requirement would be inconsistent with Congress' clear intent to preserve capabilities available to law enforcement prior to CALEA's

passage. Law enforcement traditionally has had the ability, when it conducts interceptions, promptly to discern, through the application of a tone to the circuit, if there is any mistake, interruption, or trouble affecting an interception delivery effort. In addition, law enforcement has had the ability to ensure that all of a subject's communications are intercepted, because it acquires sufficient signaling information to know that law enforcement is monitoring the correct subscriber.

96. The TIA interim standard does not recognize any affirmative obligation on the part of carriers to assure law enforcement that the carriers' equipment is operational. Yet absent mechanisms to ensure that a carrier's equipment is functioning, law enforcement will not be able to verify the efficacy, accuracy, and integrity of its surveillance. Without such mechanisms, all intercepted evidence will be subject to challenge as incomplete or inaccurate. Because the TIA interim standard imposes no obligation on carriers to "ensure" that their equipment is capable of isolating and delivering all relevant communications and call-identifying information within the scope of a surveillance order, the standard is deficient under CALEA.

97. In principle, carriers can provide law enforcement with necessary surveillance status information by a variety of means. In practice, the most efficient and reliable means is through the automated delivery of status reporting messages. The proposed rule therefore calls for the automated delivery of three kinds of surveillance status signals: (i) a continuity tone or signal, which would ensure that law enforcement is notified immediately if the delivery channels from the carrier have failed; (ii) a surveillance status message, which would verify that the surveillance is on the correct service and is operational; and (iii) a message reporting any changes in the service features of a

subscriber that might affect law enforcement's ability to obtain all of the communications it is entitled to acquire under a court order or other lawful authorization. The automated delivery of these signals is not the only means by which of the requirements of Section 103 could be satisfied, but it is the most practical and cost-effective means and therefore should be included in the technical requirements and standards established by the Commission. The provision of these signals will preserve law enforcement's ability, when a switch- or network-based interception is controlled by the carrier, to verify and document that all of a subject's calls and call-identifying information are being intercepted and "expeditiously" delivered.

98. (i) Continuity tone. Law enforcement can verify and document that all of a subject's calls were intercepted only if it has a means to discern promptly an interruption in an interception. The proposed rule provides for carriers to deliver "a continuity check in the form of an in-band signal * * * or tone * * * that will verify that CCCs [call content channels] between the carrier and a law enforcement agency are in working order." Appendix 1 (§ 64.1708(h)). As noted, law enforcement has the ability to deliver such a tone itself today when it conducts interceptions. If such a capability is not preserved, law enforcement will lose the ability automatically to verify the efficacy, accuracy, and integrity of an interception effort.

99. (ii) Surveillance status message. Today, law enforcement employs non-automated means to determine whether the interception device is accessing the correct equipment, service, or facility. However, digital switching will preclude law enforcement from performing this function because law enforcement will no longer have access to the intercept location. The proposed rule therefore

provides for the automated delivery of surveillance status messages. Appendix 1 (§ 64.1708(f)). The rule provides for surveillance messages to be triggered and delivered "whenever a surveillance is activated, updated, or deactivated," and "periodically from once every hour to once every 24 hours for the duration of a surveillance." Id. § 64.1708(f)(1)-(2). The receipt of surveillance status messages would indicate that the interception is working correctly and is accessing the correct subscriber's service. It would also confirm that the path over which the message was sent is still operational. Without this information, law enforcement would not know when the software is turned on or off, or if it has failed. Law enforcement could not verify that the subject is being monitored, leaving open the possibility that important evidence is being lost. Providing this message will enable law enforcement to quickly correct any faults in the implementation of an interception.

100. Absent an automated surveillance status message, an interception could be overridden inadvertently or removed by carrier personnel for hours or days without law enforcement's knowledge. This circumstance could occur even with a continuity check because the continuity tone applies to the status of a call content channel or circuit, while the surveillance status message applies to the operation of the surveillance software in the switch. Thus, without surveillance status messages, law enforcement could receive an active circuit without being able to confirm that the surveillance software itself was activated and functioning properly. Further, if the subjects of surveillance cease their service or change their telephone numbers, law enforcement would be unable to obtain continuous surveillance coverage or could be put in the position of monitoring the telecommunications of an uninvolved third party.

101. (iii) Feature status message. The proposed rule also provides for automated delivery of messages indicating changes in a subscriber's call features and services (e.g., conference calling and call forwarding). Appendix 1 (§ 64.1708(g)). The provision of an appropriate automated message would enable law enforcement to procure the number of delivery channels or circuits required to ensure that the interception is fully effected and delivered as authorized. Whenever a subscriber has call forwarding or other features permitting the subscriber or another person to make multi-party calls, law enforcement must have access to multiple call content channels to ensure that it will receive all communications and call-identifying information that are subject to a court order or other lawful authorization. Without knowing what features are activated on a subscriber's service, law enforcement cannot know how many interception delivery channels and circuits are necessary. And without adequate delivery circuits, call content and call-identifying information evidence will be lost.

102. A carrier that fails to provide information on changes in a subscriber's calling features or services, in a timely manner, fails to satisfy its obligation under Section 103 to "ensure" that its equipment is capable of delivering all communications and associated call-identifying information to law enforcement. Law enforcement historically has been able to obtain this kind of information, but it has had to do so through relatively slow manual means. Because there were relatively few services or features a subscriber could choose that would affect the number of delivery channels needed for an interception effort, the fact that law enforcement received information on service changes by manual means did not significantly impair law enforcement's surveillance capabilities. In today's digital environment, however, the need for prompt notification is acute, because digital

switching has enabled customers to make rapid and instantaneous changes in their services and features, and because so many services and features trigger the need for multiple delivery channels.

103. As a practical matter, the automated nature of the foregoing features is extremely important. It would be impractical both for law enforcement and for telecommunications carriers themselves if carriers were to attempt to meet their obligations under Section 103 through a system that relied upon extensive human intervention. Under such an approach, law enforcement officials would have to contact carrier employees on a daily or hourly basis to verify these aspects for every electronic surveillance effort underway. By contrast, automating these functions would provide the information promptly and without human intervention, thereby lessening the burden on law enforcement and carriers and reducing the likelihood that critical communications and call-identifying information will be lost. Therefore, while the automated delivery of surveillance status messages is not the only possible means by which carriers can meet their obligations under Section 103, the automated surveillance status message provisions of the proposed rule represent the most appropriate way to "meet the assistance capability requirements of section 103 by cost-effective methods" (47 U.S.C. § 1006(b)(1)).

104. (e) Standardization of delivery interface protocols. In order for call content and call-identifying information to be delivered from a carrier to law enforcement, the parties must use equipment with a common delivery interface protocol. Section 103 does not obligate carriers to use any particular interface protocol, and the Department of Justice and the FBI are not asking the Commission to impose such an obligation by rule. However, a limitation on the number of interface

protocols is necessary to "ensure" that, as a practical matter, all content and call-identifying information to which law enforcement is entitled can actually be delivered. Unless a relatively small number of standardized protocols are employed, each carrier will be free to employ a separate interface protocol, and law enforcement agencies could be faced with prohibitive practical and financial burdens in equipping themselves to deal with scores of different protocols. As a practical matter, law enforcement agencies thus would be denied access to information to which they are guaranteed access by CALEA.

105. Although the interim standard contains non-binding information regarding the delivery interface protocols preferred by law enforcement, it does not contain any limitation on the number of protocols that may be used by carriers to deliver call content and call-identifying information. The proposed rule limits the number of interface protocols to no more than five. Appendix 1 (§ 64.1708(j)). Within this limit, the proposed rule leaves industry free to determine for itself which interface protocols will be used. While we are proposing a limit of five protocols, we do not mean to suggest that five is the only reasonable limit. The adoption of some reasonable limit, however, is necessary to ensure that the capability assistance requirements of Section 103 are not rendered illusory in practice by a proliferation of protocols.

3. The Technical Requirements and Standards of the Proposed Rule Satisfy the Criteria of Section 107(b) of CALEA

106. As noted above, Section 107(b) of CALEA identifies a number of criteria to be considered by the Commission in establishing technical requirements and standards. The provisions of the proposed rule meet each of these statutory criteria.

107. (a) Section 107(b)(1). The first criterion of Section 107(b) is that the technical requirements and standards "meet the assistance capability requirements of section 103" and do so by "cost-effective methods." 47 U.S.C. § 1006(b)(1). The foregoing discussion demonstrates that the provisions of the proposed rule meet Section 103's assistance capability requirements. In some instances, the requirements of the proposed rule embody the only means by which Section 103's requirements can be fully met. In other instances, while more than one mechanism or requirement might suffice to discharge a carrier's assistance obligations, the interim standard fails to mandate any such mechanism or requirement at all, and the proposed rule identifies a reasonable means of ensuring that those capability requirements are met.

108. The Department of Justice and the FBI further believe that the provisions of the proposed rule represent cost-effective means of meeting the assistance capability requirements of Section 103. A precise assessment of the cost-effectiveness of the proposed rule depends in part on cost information that industry, rather than law enforcement, possesses. However, during the course of discussions between law enforcement and industry over the development of standards to implement of Section 103, industry has not identified less expensive means of obtaining the results that law

enforcement believes to be required by CALEA. If it emerges during the course of this rulemaking proceeding that there are less costly alternatives that are equally effective in terms of carrying out the assistance capability requirements of Section 103, the Department of Justice and the FBI would not object to the incorporation of such alternatives in the technical requirements and standards established by the Commission.

109. In some respects, such as the selection of a limited number of standardized delivery interface protocols (part III.A.2.e supra), adoption of the proposed rule should affirmatively reduce the overall cost of implementing CALEA to industry as well as law enforcement. Moreover, many of the capabilities requested by law enforcement in this petition would merely build upon features commonly used by telecommunications carriers today in the provision of services to customers, and could therefore be implemented at incremental cost to the carriers. For example, a carrier that supports a conference calling capability uses software to keep track of who is part of a conference call and to maintain the call through conferencing bridging equipment. If a carrier already has the ability to monitor when parties are added to, placed on hold during, or dropped from the conference call, a requirement that the carrier deliver that information to law enforcement will not impose a significant cost burden. Similarly, to route calls and for billing purposes, carriers receive and interpret subject-initiated dialing activity that directs a call through the carrier's network or allows the subject to control call services. In this regard, law enforcement simply seeks access to information that the carrier necessarily processes and maintains. In addition, in seeking notification messages reflecting network-generated signaling information, law enforcement is simply asking

carriers to transmit to law enforcement information that carriers' software is already fully capable of delivering to the carriers themselves or transmitting to their subscribers.

110. **(b)** Section 107(b)(2). The second criterion in Section 107(b) is that the technical requirements and standards "protect the privacy and security of communications not authorized to be intercepted." 47 U.S.C. § 1006(b)(2). The capabilities and features in the proposed rule in no way jeopardize these privacy and security interests. As explained above, Title III contains numerous provisions designed to ensure that lawful surveillance does not unnecessarily intrude on the privacy of communications that are outside the legitimate scope of the criminal investigation, and CALEA itself contains additional privacy safeguards. See, e.g., 18 U.S.C. § 3121(c) (as amended by Section 207(b) of CALEA); 47 U.S.C. § 1002(a)(4)(A). In important respects, the provisions of the proposed rule actually enhance these privacy protections. For example, information on participants in a multi-party call that is conveyed by party hold and party join messages enhances privacy because law enforcement can more readily avoid recording conversations that are not of a criminal nature. Similarly, receipt of surveillance status messages ensures that the interception software is working correctly and is not accessing the service of an innocent subscriber. And the delivery of all call-identifying information, including post-cut-through dialed digits, over a call data channel would obviate the need to access a call content channel when law enforcement agencies are seeking only call-identifying information.

111. **(c)** Section 107(b)(3). The third criterion in Section 107(b) is that the technical requirements and standards "minimize the cost of * * * compliance on residential ratepayers." 47 U.S.C.